Privacy Impact Assessment (PIA)

Name of Project: Microfiche Reader Modernization Project

Project's Unique ID: MRMP

Legal Authority(ies):	**OPM's authority to require agencies to collect this information is established in Title 5, Section 2951 of the U.S. code (5 U.S.C. 2951) and Title 5, Part 9.2 of the Code of Federal Regulations (5 CFR 9.2). NARA's obiligations to protect this information is provided in NARA Directive 1608, the Privacy Act of 1974 (Pub. L. 93-579, 88 Stat. 1896, enacted December 31, 1974, and 5 U.S.C. 552a), a United States Federal Law.**

Purpose of this System/Application: Commercial Off The Shelf (COTS) microfiche system which allows for high speed conversion of the microfiche images into a digital file and applies smart recognition software which auto adjusts the images for focus, contrast, and orientation. The system consists of a high speed scanner, smart software, monitors, PCs, and high speed printers.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Employees		N/A. The information system will not collect information about National Personnel Record Center (NPRC) employees who use the system other than logon information and user actions performed on the system.
External Users		N/A. There will be no external users of the information system.
Audit trail information (including employee log-in information)		Audit records of logins and user actions will be captured on the system.
Other (describe)		The digital files captured by the system will be of military personnel records currently maintained as microfiche images. These microfiche images contain Personally Identifiable Information (PII). The data elements contained within these military personnel records include veteran name, date of birth, social security number (SSN), service history, and medical history while in service.

Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

NARA operational records		The digital files created by the system will be of military personnel records currently maintained as microfiche images. These micorfiche images contain PII.
External users		N/A. Data elements will not be obtained from external users of the information system.
Employees		The only employee information that will be captured by the system will be logon information and users actions within the system during the performance of their job responsibilities.
Other Federal agencies (list agency)		N/A. Data elements will not be obtained form other Federal agencies.
State and local agencies (list agency)		N/A. Data elements will not be obtained form state and local agencies.
Other third party source		N/A. Data elements will not be obtained form other third party sources.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

Many military personnel records are stored exclusively on microfiche. The digital conversion and printing of microfiche images are required by NPRC in order to satisfy customer requests for these files.

2. **Is there another source for the data? Explain how that source is or is not used?**

Many military personnel records are stored exclusively on microfiche. The source microfiche is used to create a digital file that can be printed out in order to satisfy customer requests for these files.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

2. Will the new data be placed in the individual's record?

N/A. See Section 3, Question 1.

3. Can the system make determinations about employees/the public that would not be possible

without the new data?
N/A. See Section 3, Question 1.

4. How will the new data be verified for relevance and accuracy?
N/A. See Section 3, Question 1.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
N/A. See Section 3, Question 1.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
N/A. See Section 3, Question 1.

7. Generally, how will the data be retrieved by the user?
Military personnel records stored on microfiche will be scanned and converted into digital pdf files. These digital files will then be printed using high speed printers. The printed hard copy will then be delivered to the requesting technician by support staff. Hard copy files will be named using the Case Management Reporting System (CMRS) Search Request Number used for the associated correspondence request.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.
No. Once converted, digital files within the system will be retrievable through the CMRS Search Request Number and/or the record's NPRC Registry Number.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
N/A. No reports are created by the system. The microfiche records are converted to digital pdf files

and then printed to hard copy using high speed printers.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
No

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.
The system will be able to identify the NPRC personnel who logged into the system and created the electronic pdf files.

12. What kinds of information are collected as a function of the monitoring of individuals?
Audit logs of NPRC personnel who access the system to perform authorized actions on the system in accordance with their job responsibilities will be captured within the server and workstation operating systems.

13. What controls will be used to prevent unauthorized monitoring?
Audit logs will only be accessible to authorized individuals through the user account permissions within the server and workstation operating systems.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
N/A. The system is not web-based.

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?
The system will be accessible by the NPRC users, leads, supervisors, managers, and management analysts who are assigned to the MRMP. It will also be accessed by NARA IT and

Telecommunications Support Services (NITTSS) personnel and by the vendor of the microfiche scanner/equipment for system administration and hardware/software technical support.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?

User access to the system will be requested by supervisors and managers assigned to the MRMP. System administrators will then set up users in the system's Active Directory and provide them with userids and temporary passwords (which will be changed by the users on first log in). Userids will deactivated/revoked by system administrators at the request of supervisors and managers when an employee no longer requires access to MRMP. User access procedures will be covered under the MRMP Account Management SOP (currently under development) and documented NITTSS standard operating procedures to manage accounts on servers and workstations that they administer.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

Digital files older than thirty days will be deleted from the system. Users will have access to all digital files of scanned microfiche records that are currently on the system after conversion as a part of their basic duties.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?

All MRMP users receive mandatory annual holdings protection training to prevent the misuse of the data contained in MRMP.

The scanning area is a restricted area that will be controlled by badge access and limited to NPRC RRB personnel and those who need access to the system. The physical access control system for the room will control access to the area and will be monitored by physical security staff.

The system will reside on an isolated Virtual Local Area Network (VLAN) on NARA's network with no access to the internet.

In order to access the system, users must have a valid userid and password. Workstations will be configured to meet standard government baseline requirements and servers will be configured to meet Center for Internet Security (CIS) benchmarks to ensure that the required level of auditing is in place.

Annual assessments of select security and privacy controls will be conducted by NARA's independent assessors at the direction of the NARA IT Security Management Division (IS).

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors are involved with the design and development of the system. Contractors will also be responsible for the maintenance of the software including patching and flaw remediation. In addition, NITTSS personnel will be responsible for the operation and maintenance, including patching and flaw remediation, of the servers, workstations, printers and scanners associated with the system.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.

No other NARA system will provide, receive, or share data in the system.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

N/A. See Section 4, Question 6.

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The NARA Senior Agency Official for Privacy (SAOP), the NARA Chief Privacy Officer (CPO), as well as the System Owner will be responsible for protecting the privacy rights of individuals identified in the military personnel records processed by the system.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

No other agency will share data or have access to the data in this system at this time.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

N/A. NPRC personnel and NITTSS personnel will have access to the system to perform required, authorized duties. The vendor of the microfiche scanner/equipment will also periodically access the system to provide hardware/software technical support. NPRC, NITTSS personnel, and vendor personnel accessing the system will be presented with NARA's approved System Use Notification banner which users will have to acknowledge prior to access.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A. NPRC personnel and NITTSS personnel will have access to the system to perform required, authorized duties. The vendor of the microfiche scanner/equipment will also periodically access the system administration and hardware/software technical support. NPRC, NITTSS personnel, and vendor personnel accessing the system will be presented with NARA's approved System Use Notification banner which users will have to acknowledge prior to access.

Section 6: Security of Collected Information

1. **How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).**

The data processed by the system will consist of digital files of military personnel files scanned from microfiche records. Smart recognition software will be used to adjust the image for focus, contrast, and orientation. The software will also allow for batch editing of multiple images.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A. The system will not operated in more than one site.

3. What are the retention periods of data in this system?

Digital images of scanned Military Personnel Records created from microfiche will be maintained for

30 days within the system.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

The microfiche copy is the official record in this instance. The digital pdf files created by the system will be temporary reference copies that are created in order to be immediately printed out to paper hard copy in order for NPRC to service record requests. The digital copy will only be kept for thirty days in the event that a re-print is needed before being manually purged from the system.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

The system will use dedicated high speed scanners and commercial off the shelf (COTS) smart recognition software to create digital images of Military Personnel Records maintained on microfiche. These digital images will than be printed on dedicated high speed printers by NPRC staff. These printed images will then be provided to customers requesting the record. This is no different from how NPRC previously employed these technologies. The only difference is that the system provides high speed conversion of the microfiche images into digital files and applies smart recognition software which adjusts the image for focus, contrast, and orientation. The software also allows for batch editing of multiple images, reduces, technician time, and improving productivity.

6. How does the use of this technology affect public/employee privacy?

Authorized NPRC personnel will utilize the system to make digital files of microfiche images to fulfill customer requests for military personnel records stored exclusively on microfiche. These files will contain PII.

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

The system is under development and will meet NARA IT Security Requirements as well as requirements of the NIST SP 800-53 Moderate Baseline. Security and privacy control implementations will be documented in the System Security Plan (SSP) and Privacy Plan.

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?
A risk assessment is scheduled to be performed as part of the initial security assessment performed by NARA's independent assessors. A Risk Assessment Report (RAR) will be prepared by the independent assessors and will be used by the NARA Designated Approval Authority (DAA) and the Senior Agency Official for Privacy (SAOP) in their determination to grant an Authorization to Operate (ATO) to the system. Mitigations for identified risks will be tracked in a Plan of Action and Milestones (POA&M) in order to ensure safeguards are in place to protect information processed by the system. Workstations will be configured in accordance with the United States Government Configuration Baseline (USGCB). Servers associated with the system will be hardened against relevant configuration benchmark guides. Physical controls will be in place to restrict access to the sysystem equipment and the system will be isolated on a VLAN on NARA's network wth no access to the internet.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
An initial security assessment is scheduled to be conducted by NARA's independent assessors. A Security Assessment Package will be prepared by the independent assessor that includes a Security Assessment Report (SAR), RAR, POA&M, and Certifier's Recommendation. Once an ATO has been granted for the system by the DAA and SAOP, and annual assessment of select security and privacy controls will be conducted by NARA's independent assessors. The SAR, RAR, and POA&M will be updated accordingly based on the results of the annual assessment. In addition to the annual assessment of security and privacy controls implemented on the system, the NARA IT Security Management Division (IS) and the Operations and Infrastructure Branch (IOO) will install and monitor NARA's continuous monitoring tools on the system. These tools will be used to scan the system for vulnerabilities and configuration compliance.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
John Coffin, john.coffin@nara.gov

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.
N/A

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
N/A

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?
No

2. If so, what changes were made to the system/application to compensate?
N/A

<u>See Attached Approval Page</u>

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
10/23/2017 X Jason Hardy Signed by: National Archives and Records Administration (Signature)	23 Oct 2017 (Date)
Name: Jason Hardy	
Title: Chief, Management Systems Staff - AFN	
Contact information: jason.hardy@nara.gov	
Senior Agency Official for Privacy (or designee)	
(Signature)	10/24/17 (Date)
Name: Gary Stern	
Title: General Counsel	
Contact information: garym.stern@nara.gov	
Chief Information Officer (or designee)	
Swarnali Halder (Signature)	11/2/17 (Date)
Name: Swarnali Haldar	
Title: Information Services Executive/Chief Information Officer (CIO)	
Contact information: swarnali.haldar@nara.gov	